## REMARKS / DISCUSSION OF ISSUES

Claims 1-20 are pending in the application.

The applicants thank the Examiner for acknowledging the claim for priority and receipt of certified copies of all the priority documents, and for advising the applicants that the drawings are accepted.

The Office action objects to the abstract; a replacement abstract is provided herein.

The Office action objects to and rejects claims 17 and 18 under 35 U.S.C. 112, second paragraph. Claim 17 is correspondingly amended herein.

The Office action rejects claims 1, 16, 17, and 19 under 35 U.S.C. 103(a) over Leighton et al. (USP 5,519,778, hereinafter Leighton) and Hoffstein et al. (USP 6,076,163, hereinafter Hoffstein). The applicants respectfully traverse this rejection.

MPEP 2142 states:

> "To establish a *prima facie* case of obviousness … the prior art reference (or references when combined) ***must teach or suggest all the claim limitations***… If the examiner does not produce a *prima facie* case, the applicant is under no obligation to submit evidence of nonobviousness."

Claim 1 claims a method of generating a common secret between a first party and a second party as a product of two symmetrical polynomials. Claims 16, 17, and 19 include similar limitations.

Neither Leighton nor Hoffstein teaches or suggests generating a common secret between a first party and a second party as a product of two symmetrical polynomials.

The Office action acknowledges that Leighton does not teach generating a common secret between a first party and a second party as a product of two symmetrical polynomials, and asserts that Hoffstein provides this teaching. The applicants respectfully disagree with this assertion. Hoffstein does not address generating a common secret between two parties.

Hoffman teaches a method for verifying the identity of a user and for providing a digital signature of the user. Hoffman's user has a secret key f(x), but this secret key is not common between Hoffman's user and any other party. The user provides a product of polynomials to a verifier, but this product cannot be considered a secret between the two, because it is the parameter that is publicly communicated to the verifier.

Further, claim 1 includes the limitation that the two symmetrical polynomials are each evaluated in a value received from the second party. Hoffman does not teach receiving two values from the user and using each of these values to determine a value of a corresponding symmetrical polynomial, from which to form the aforementioned product corresponding to a secret between the parties.

Because neither Leighton nor Hoffman, individually or collectively, teaches or suggests generating a common secret between a first party and a second party as a product of two symmetrical polynomials that are each evaluated in a value received from the second party, the applicants respectfully maintain that the rejection of claims 1, 16, 17, and 19 under 35 U.S.C. 103(a) over Leighton and Hoffstein is unfounded, per MPEP 2142, and should be withdrawn.

The Office action rejects:

claims 2-3 and 9-12 under 35 U.S.C. 103(a) over Leighton, Hoffstein, and Matyas et al. (USP 5,953,420);

claims 13-15 under 35 U.S.C. 103(a) over Leighton, Hoffstein, and Menezes et al. (Handbook of Applied Crytography, ISBN 0-8493-8523-7); and

claim 18 under 35 U.S.C. 103(a) over Leighton, Hoffstein, and Oishi (USP 6,298,153). The applicants respectfully traverse this rejection.

Each of the rejected claims are dependent upon independent claims 1, 16, or 17, and in each of these rejections, the Office action relies upon Leithton and Hoffstein for teaching the elements of these independent claims.

As noted above, neither Leighton nor Hoffman teaches or suggests each of the elements of claims 1, 16, or 17. Accordingly, the applicants respectfully maintain that the rejections of claims 2-3, 9-15, and 18 under 35 U.S.C. 103(a) that rely upon Leighton and Hoffman for this teaching are unfounded, per MPEP 2142, and should be withdrawn.

In view of the foregoing, the applicants respectfully request that the Examiner withdraw the rejections of record, allow all the pending claims, and find the application to be in condition for allowance. If any points remain in issue that may best be resolved through a personal or telephonic interview, the Examiner is respectfully requested to contact the undersigned at the telephone number listed below.

Respectfully submitted,

/Robert M. McDermott/

Robert M. McDermott, Esq.
Registration Number 41,508
Phone: 804-493-0707
Fax: 215-243-7525

**Please direct all correspondence to:**
Larry Liberchuk, Esq.
Philips Intellectual Property and Standards
P.O. Box 3001
Briarcliff Manor, NY 10510-8001
Phone: (914) 333-9618
Fax: (914) 332-0615